N61340-17-R-0003
Attachment J-1 SOW Rev-3
28 November 2018

STATEMENT OF WORK
FOR
Software Maintenance of Fielded Training Systems
(SWMFTS)

NAVAL AIR WARFARE CENTER
TRAINING SYSTEMS DIVISION
12211 Science Drive
Orlando, Florida 32826-3224

PREPARED BY: _____ **DATE:** _____
JOHNNY TRUETT
Branch Head
AIR-4.6.4.2

APPROVED BY: _____ **DATE:** _____
JOHN SHAW
Division Head
AIR-4.6.4

Revision Number	Purpose	Date
Rev-1	Update the Appendix B Labor Mix Hours for the 5 month reduction in the Period 1 Period of Performance.	11-Jan-2018
Rev-2	Update the Appendix B Labor Mix Hours for the 4 month reduction in the Period 1 Period of Performance.	19-Jun-2018
Rev-3	Update the Appendix B Labor Mix Hours for the additional 4 month reduction in the Period of Performance.	28-November-2018

Table of Contents

Statement of Work For
Software Maintenance of Fielded Training Systems

1. Applicable Documents.

This Statement of Work (SOW) conforms to policy in the documents listed herein. Nothing in this SOW supersedes applicable laws and regulations.

Title 5 of the U.S. Code, Section 552.a - Privacy Act of 1974. (http://uscode.house.gov/search /criteria.shtml).

Applicable Cyber Security Directives, Instructions, and Guidance. All Cyber Security shall be in compliance with the following listed instructions to include those referenced within the below listing:

a. The National Security Act of 1947.

b. Title 40/Clinger-Cohen Act.

c. OMB Memorandum M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, September 14, 2011.

d. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01I (series), Joint Capabilities Integration and Development System, 23 January 2015.

e. CJCSI 6211.02D (series), Defense Information System Network (DISN): Policy and Responsibilities, 24 January 2012, Current as of 4 August 2015.

f. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011, Current as of 9 Jun 2015.

g. CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012, Current as of 18 December 2014.

h. Defense Acquisition Guidebook – Chapter 7, Acquiring Information Technology, Including National Security Systems, Section 7.5, Information Assurance (IA).

i. DoD 5200.2-R, Personnel Security Program," January 1, 1987, as amended.

j. DoDD 8000.01, Management of the Department of Defense Information Enterprise, February 10, 2009.

k. DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004, Certified Current as of 23 April 2007.

l. DoDD 8500.01, Cybersecurity, March 14, 2014.

m. DoDD 8140.01, Cyberspace Workforce Management, August 11, 2015.

n. DoDI 8100.04, DoD Unified Capabilities (UC), December 9, 2010.

o. DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), May 21, 2014.

p. DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, November 3, 2009.

q. DoDI 8510.01, Risk Management Framework (RMF) For DoD Information Technology(IT), March 12, 2014.

r. DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, May 24, 2011.

s. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), May 28, 2014.

t. DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 2005 (Incorporating Change 3, January 24 , 2012).

u. DoDI 8580.1, Information Assurance in the Defense Acquisition System, July 9, 2004.

v. DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, June 8, 2010.

w. DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, June 6, 2012.

x. DoD 5220.22-M, National Industrial Security Program Operating Manual, February 28, 2006 (NISPOM) with Change 1, March 28, 2013.

y. CNSS Policy No. 11, National Policy Governing The Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, Jun 10, 2013.

z. Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems, March 27, 2014, as amended.

aa. SECNAV M-5239.1, Department of the Navy Information Assurance Program; Information Assurance Manual, November 2005.

bb. SECNAVINST 5230.15, Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software, 10 April 2009.

cc. SECNAVINST 5239.3B, Department of the Navy Information Assurance Policy, June 17, 2009.

dd. SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements, 18 March 2008.

ee. SECNAVINST 5239.20, DON Cybersecurity/Information Assurance Workforce Management, Oversight and Compliance.

ff. SECNAV5239.2- Ml, Cybersecurity Workforce Management and Qualification Manual (Draft).

gg. Department of Defense Information Technology Portfolio Repository- Department of the Navy (DITPR-DON) Registration Guidance, December 5, 2011.

hh. Federal Information Processing Standard Publication (FIPS Pub) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

ii. National Institute of Standards and Technology (NIST) 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010.

jj. NIST Special Publication 800-60 Volume 1 Revision 1, Volume I: Guide to Mapping Types of Information and Information Systems to Security Categories, August 2008.

kk. NIST Special Publication 800-60 Volume 2 Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

ll. NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 30, 2013.

mm. NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.

nn. NIST Special Publication 800-137 Revision 1, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011.

oo. NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003.

pp. Space and Naval Warfare (SPAWAR) Memorandum, Qualification Standards and Registration Procedures for Navy RMF Validators, DRAFT.

qq. Navy Authorizing Official (AO) and Security Control Assessor (SCA) Risk Management Framework Process Guide, 31 August 2015.

rr. DON CIO Memo 02-10, Department of the Navy Chief Information Officer Memorandum 02-10 Information Assurance Policy Update for Platform Information Technology, 26 April 2010.

ss. Office of the Chief of Naval Operations Instruction (OPNAV INST) 5239.1C, Navy Information Assurance (IA) Program, 20 Aug 08.

tt. Chief of Naval Operations/Headquarters, United States Marine Corps, CNO N614/HQMC C4 - Navy-Marine Corps Unclassified Trusted Network Protection (UTN-Protect) Policy, Version 1.0, 31 October 2002.

2. Scope.

In accordance with DoDD 8500.1 training simulators and training systems employing computer resources, both hardware (HW) and software (SW), that are physically a part of, dedicated to, or essential in real time to the mission performance of special-purpose Information Technology (IT) Systems are platforms. The IT embedded in the training system is called Platform IT. This SOW establishes the NAWCTSD requirements for Software Maintenance of Fielded Platform IT Training Systems at 16 sites in CONUS and overseas. Support includes operation, maintenance, and repair of trainer Platform IT consisting primarily of corrective, adaptive, perfective and preventative SW maintenance; some limited HW operation, maintenance, and repair; and associated minor support tasks. Training System modifications may also be incorporated as applicable. The trainers simulate aviation, surface, and undersea platforms and they include: operator training systems, weapons training systems, training environments, use of sensors, and communications network systems. Locations for support are at military facilities in CONUS and overseas.

3.0 Requirements.

3.1 General Requirements.

This SOW requires the Contractor to provide primary O&M, N funded SW Maintenance and HW O&M tasks, and minor support tasks that are Professional Engineering and Technical tasks in support of the primary tasks. Minor support tasks include configuration management, technical support, engineering change plan support (ECP), Integrated Project Team (IPT) support, Fleet Synthetic Training (FST) support, and Cyber Security support of training devices, documentation support, and supply support for the purchase and installation of incidental material, as well as the associated management and administrative support. The Contractor is required to perform all applicable Cyber Security functions in Appendix C in association with the tasks listed below.

3.1.1 Platform IT SW Maintenance and HW O&M Support.

The contactor shall provide personnel to ensure 100% of daily requirements for the operation, maintenance, and repair of trainer Platform IT. The Contractor shall employ only fully qualified personnel who meet the qualifications provided under Appendix A to perform the tasks specified in this SOW. The COR will review resumes of Contractor personnel performing support to ensure they meet the contractual requirements. Each person is subject to verification to ensure

that they meet the proposed category descriptions. During the period of performance, the Contractor shall employ personnel in a manner that maximizes productivity and efficiency ensuring that no positions are open longer than 60 days.

3.1.1.1 Place of SW Maintenance of Fielded Platform IT Training System Performance. Contractor shall support training systems at military facilities in CONUS and overseas. Current sites where NAWCTSD requires support are:

Norfolk VA	Oceana VA	Newport RI	Cherry Point NC
Kingsville TX	Jacksonville FL	Pensacola FL	Miramar CA
Camp Pendleton CA	San Diego CA	Whidbey Island WA	Iwakuni Japan
Atsugi Japan	New River NC	Yuma AZ	North Island CA

During the period of performance, other locations may require support in CONUS or overseas. Note: The Government will not provide reimbursement for Permanent Change of Station, lodging, or travel costs associated with permanent relocation. The Government has the ability to provide the required spaces at its facility for this effort. The Government will provide the office spaces, desks, chairs, computers, printers, paper and pens that are necessary for the performance of this task order.

3.1.2 Other Direct Costs (ODCs).
All Travel, Materials and Shipping purchases will be made on a COST reimbursable CLIN, reimbursable at COST plus G&A only when funding has already been provided. The Government will be the final acceptance authority for all products and services.

3.1.2.1 ODCs for Materials and Shipping.

All material necessary to complete scheduled work requirements will be provided via the DOD supply system to the maximum extent possible. When material and shipping cannot be provided by the Government in time to meet established scheduled requirements the Government may authorize the Contractor to purchase the required item or shipping. Incidental Materials and Shipping include the purchase or repair of items incidental to the Platform IT SW and HW O&M Support including, but not limited to, damaged end items, damaged components, parts, batteries, memory, repair kits, hard drives and SW licenses. This substantially reduces wait times for trainers and reduces costs to the Government for additional contracting of required individual small items that can stop training. The Government may provide the Contractor with authorization to utilize Federal Supply Schedules for commercial material purchases in accordance with FAR Clause 52.251-1. All incidental material and shipping purchases will be approved in accordance with NAVAIR Clause 5252.242-9515 RESTRICTION ON THE DIRECT CHARGING OF MATERIAL.

3.1.2.2 ODCs for Travel.

The Government ISEO will inform the Contractor when travel is necessary to accomplish a task. All travel requests will require prior COR approval. Government Directed travel shall be reimbursed IAW Joint Travel Regulation Requirements (JTR). The Government will not provide reimbursement for Permanent Change of Station, lodging, or travel costs associated with

permanent relocation. All Travel Materials and Shipping purchases require Government pre-approval. All Travel will be approved in accordance with NAVAIR Clause 5252.232-9509 TRAVEL APPROVAL AND REIMBURSEMENT PROCEDURES.

3.1.3 Contractor Management.

The Contractor shall organize, coordinate, and control all Contractor activities to ensure compliance with contract performance, cost, and schedule requirements. The Contractor shall monitor the progress of all work performed and all costs incurred under the contract. The COR or Project Manager may request that the Contractor provide a Plan of Action and Milestones (POA&M) for task completion. The POA&M shall define the Contractor's methods and schedule for implementing the tasks as specified in this SOW. The Contractor shall furnish the POA&M as part of the Contractor's Progress, Status, and Management Report. The Contractor shall prepare the Contractor's Progress, Status, and Management Report in accordance with the Contract Data Requirements List (CDRL, B001).

3.1.3.2 Mobilization.

The Contractor shall achieve full performance responsibility within 60 days after contract award and ensure a smooth transition of responsibilities. Contractor staffing shall be 100% complete within 60 calendar days after contract award. The Contractor shall conduct a joint (NAWCTSD COR/Contractor) mobilization meeting within one week after Contract Award to discuss execution of Mobilization, the respective responsibilities of all parties, and the Contractor's readiness to assume full performance duties. The joint meeting will be conducted at a site and time as selected by the COR. The Contractor shall prepare meeting minutes for the mobilization meeting in accordance with the Contractor Provided Meeting Minutes Format Contract Data Requirements List (CDRL, B002).

3.1.3.3 Transition.

The Contractor shall ensure an orderly transition of contract responsibilities to the successor Contractor during the last 30 calendar days of contract performance and minimize impact on the Government. As an On-the-Job Training (OJT) function throughout the transition phase, the Contractor shall allow the successor contractor to observe (over-the-shoulder) the performance of all SOW efforts.

At the end of the contract period of performance the Contractor shall keep the Government fully informed of status throughout the transition period. Throughout the transition period, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The Contractor shall cease operations and vacate all facilities by 2400 (midnight) on the last day of contract performance, unless agreed upon in advance by the Contracting Officer.

3.1.4 Emerging APN Projects.

Emerging APN Projects consist of Training System Modifications. Emerging APN requirements may arise over the course of the contract and may be negotiated and incorporated as applicable in accordance with DFARS Clause 252.217-7028 OVER AND ABOVE WORK and NAVAIR Clause 5252.217-9507 OVER AND ABOVE WORK REQUESTS (OAWR). Emerging APN Projects are short duration efforts funded with APN appropriations. A PSC determination will

be made at the time of incorporation based on the particular Emerging APN Project requirements. A particular Emerging APN Project may take place at one or more of the site locations in SOW 3.1.1.1. Emerging APN Projects are needed to maintain training system integrity but do not add new training system capabilities. Typical Emerging APN Projects include but are not limited to: Safety modifications, Computer Operating System upgrades, and Engineering Change Proposals (ECPs). The SOW will be updated with the Emerging APN Modification OAWR requirement SOW Addendums under Appendix D.

3.1.5 Administrative Support.
The Contractor shall meet the administrative standards in the following sub-paragraphs:

3.1.5.1 Post Award Conference.
The Contractor shall hold a Post Award Conference two weeks after award to establish the framework of the Contractor and Government interaction during the performance period of the contract. The Contractor shall prepare meeting minutes for the Post Award Conference in accordance with the Contractor Provided Meeting Minutes Format Contract Data Requirements List (CDRL, B002).

3.1.5.2 Non-Personal Services.
The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances will the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the PCO immediately.

3.1.5.3 Personnel Appearance and Conduct.
Contractor personnel performing on a military reservation shall comply with all applicable rules, regulations, directions, and requirements pertaining to conduct of personnel on a military reservation. The Contractor shall recognize the authority of the military Commander to suspend, restrain, or restrict the activities of Contractor personnel for the protection of personnel and equipment under his military jurisdiction. Contractor personnel shall wear a Contractor-provided identification badge and a "Navy Contractor Badge" while performing work for the Navy. Contractor personnel shall identify themselves as a Contractor in all verbal and written communication means while performing work for the Navy. When attending meetings in support of the Navy, Contractor personnel shall introduce themselves as a Contractor employee working for the Navy. Contractor personnel shall sign a non-disclosure statement relative to Government business sensitive information.

3.1.5.4 RESERVED.

3.1.5.5 RESERVED.

3.1.5.6 Computer Proficiency.
As a minimum, all Contractor personnel shall be proficient in the use of electronic and SW tools including Microsoft Office. Personnel shall rapidly learn to use any new electronic tools or SW tools provided.

3.1.5.7 Conferences and Meetings Support.
The Contractor shall attend meetings, generate minutes, and/or track action items generated using a Government approved tracking system. The Contractor shall prepare meeting minutes in accordance with the Contractor Provided Meeting Minutes Format Contract Data Requirements List (CDRL, B002). The Contractor shall provide status of action items in the Contractor's Progress, Status, and Management Report (CDRL, B001).

3.1.5.8 Delivered Data.
Data shall be delivered IAW the attached CDRLs, DD Forms 1423, which cite the DIDs or other appropriate reference for technical data and other information required during the performance of this contract.
CDRL B001: DI-MGMT-80227 Contractor's Progress, Status, and Management Report
CDRL B002: DI-ADMN-81505 Contractor Provided Meeting Minutes Format
CDRL B003: DI-MGMT-80934C Contractor's Operational Security Plan

3.1.5.9 Government Documents and Information.
The Government will provide all necessary reference documents not generally available to the Contractor as required. Throughout the life of the contract, if any instruction or document is replaced or superseded, the replacement or superseding instruction or document shall be applicable to the requirements defined in this SOW.

3.1.5.10 NMCI Services for Contract Performance.
The Government will provide the Contractor with any NMCI services and assets as required for the performance of this contract. The COR will place NMCI orders with the NMCI Contractor. The COR will coordinate NMCI support through NAWCTSD 7.2.4.

3.1.5.11 Safety Standards.
Contractor personnel, although recognized as employees under the administrative control of the Contractor, shall comply with the directives and requirements of the local base Commander regarding safety standards and security regulations while working on or at a Government facility. Contractor personnel shall be subject to safety and security inspections and investigations at all times. Contractor personnel shall immediately report any accident/incident with safety/security implications or any other conditions or incidents that could be reasonably expected to be of interest to the Government. Initial reports may be verbal, but shall be followed up in writing within twenty-four (24) hours. All reports shall be forwarded to the COR.

3.1.5.12 PKI Certification.
The Government will provide PKI Certification for Contractor personnel, if necessary.

3.1.5.13 Passports.

Contractor personnel required to support travel for overseas site surveys shall obtain passports within 2 weeks of required travel dates (Assumes 60 day prior to travel notification by the Government).

3.1.5.14 Working Hours.

The Contractor shall provide the services and staffing necessary to successfully perform tasks specified in this SOW. Work schedule may vary across locations. The Contractor shall provide support personnel in accordance with the following parameters:

a. Core Work Hours (CWH): CWHs vary from 8 to 9 hours daily (not including a 30-minute lunch-break), to start as early as 0600 and end as late as 1800 Monday-Friday. Services and staffing shall be provided for each office at least 8 hours per day (excluding the 30 minute lunch break). CWHs may include a "Compressed Work Schedule" (CWS), which is an alternative work schedule to the traditional five 8-hour workdays per week. Under a CWS an employee completes the following schedule within a two-week period of time: eight weekdays are worked at 9 hours each, one Friday is alternately worked as 8 hours and one Friday is not worked. The result is 80 hours worked every two weeks, with 44 work hours one week and 36 hours the other. The Contractor, with agreement by the COR, may allow its employees to work a CWS schedule (typically matching that of local Government employees). Any Contractor that chooses to allow its employees to work a CWS schedule in support of this contract agrees that any additional costs associated with the implementation of the CWS schedule vice the standard schedule are unallowable costs under this contract and will not be reimbursed by the Government.

b. Non-Core Work Hours (NCWHs): These are hours worked outside any CWH schedule as defined above. These hours include those between 1800 and 0600 Monday-Friday and on Weekends. Approximately 25-50% of the required work is anticipated to occur during NCWHs. Specific work schedule and/or requirements shall be provided via an addendum at the time of award.

3.2 Detailed Requirements.

The following sections define the tasks that the Contractor shall accomplish in support of NAWCTSD SW Maintenance of Fielded Platform IT Training Systems. The Government will not assign tasks to, or prepare work schedules for individual Contractor employees. All tasks will be assigned to the Contractor who will assign tasks to Contractor employees for performance. The Contractor shall provide effective technical support and accurate tracking for the work tasks detailed in this section.

In all of the following tasks the Contractor's role is to assist the Government with activities such as coordinating, collecting, analysis, and reporting. The Contractor will make recommendations to the Government, but will not make decisions. The Government reviews the Contractor's input and is responsible for decision-making especially pertaining to determining the Government Property to be disposed of and on what terms, determining the supplies or services to be acquired by the Government, evaluating another Contractor's performance, acquisition planning, technical evaluations of Contractor proposals, and development of statements of work.

3.2.1 Primary Tasks: O&M,N Funded Tasks (PSC J069 Maintenance & Repair of Training Aids & Devices; OCC 257 O&M)

3.2.1.1 SW Maintenance Support.
The Contractor shall assist the Government In Service Engineering Office (ISEO) with SW maintenance support efforts including corrective SW maintenance (fixing SW errors), adaptive SW maintenance (adapting SW to new environments, HW, or operating systems), perfective SW maintenance (implementing new or changed SW functionality) and preventative SW maintenance (preventing the occurrence of SW errors, code optimization, document updating, and code restructuring). The Contractor shall support the design, development, implementation, and documentation of Modeling and Simulation (M&S) systems, SW, research efforts, and related processes including system interoperability. The contractor may perform documentation support, IPT support and configuration management support that is incidental and integral to the SW Maintenance support tasks. Specific SW Maintenance support may include but not be limited to:

a. Developing SW using high order languages that is efficient, readable, and well documented.

b. Preparing reports describing status of SW under development.

c. Suggesting solutions to problems that arise during the development or modification of simulation related real-time computational systems.

d. Analyzing requirements and preparing a SW design approach for proposed training system(s). Provide alternative design approaches with tradeoff analyses and risk assessments.

e. Conducting analyses to ensure that SW designs are cost effective and satisfy requirements.

f. Providing support developing software specifications detailing design, expected performance, testing, and provisions for SW acceptance.

g. Reviewing SW design and conduct code reviews.

h. Monitoring and adhering to the SW configuration management practices.

i. Identifying problems encountered in SW development and providing recommendations as to how to resolve these problems.

j. Providing support in developing test plans and when needed, providing support in performing examinations and acceptance tests.

k. Actively maintaining and enhancing job related knowledge and skills in M&S, SW development techniques, state-of-the-art computer architectures, emerging technologies, and other SW development areas.

l. Applying decision analysis techniques to ensure that the engineering approach satisfies the training objectives.

3.2.1.2 HW O&M Support.
The Contractor shall assist the Government ISEO with HW development operation, maintenance and repair efforts. These include: design, prototype, manufacture, installation, modification, and testing of training device mechanical, electrical, electronic, optical, and electro-mechanical components and systems.

3.2.1.3 Computer/Electronics Support.
The Contractor shall support computer/electronics efforts for training and simulation systems for programs as follows:

a. Developing SW and HW techniques for simulation, training, and simulation-based acquisition applications.

b. Support preparation of technical specifications and procurement data for advanced studies and developments. Attend bidder conferences to explain the requirements of the contract and to answer questions pertaining thereto.

c. Recommend most suitable technical approach taking into consideration proposed approach to problem, personnel, and facilities to be used. Monitor and evaluate the progress of applied research and advanced development requiring the application of new techniques or methods. Render solutions concerning the applicability of technical methodology used, degree of conformance to requirements, and overall project performance.

d. Maintain current awareness of technological developments in the use of computer SW and HW in the technology base for simulation, modeling, and training research investigations. Evaluate technology to predict and optimize effectiveness in training systems; e.g., scene rendering SW, graphics accelerators, database modeling SW and techniques, sensor simulation integration, human animated characters, and weapon tracking systems.

3.2.2 Minor Support Tasks: O&M,N Funded Tasks (PSC R425 Professional Engineer Services; OCC 251 Advisory & Assistance Services).

Minor Support Tasks are ancillary tasks that may be performed in support of the Primary O&M,N funded tasks in section 3.2.1 above.

3.2.2.1 Cyber Security and Network and Computer Systems Support.
The Contractor shall assist the Government ISEO in the administration, general maintenance and Cyber Security of networks and computer systems HW and SW for assigned training devices and off-line development systems. The Contractor shall collect, organize, and analyze network and computer systems data.

3.2.2.2 Cyber Security and Network and Computer Systems Administration Support for Level I Computing Environments.

Level I Computing Environments are defined in DoD 8570.01-M. The Contractor shall assist the Government ISEO by providing appropriately certified personnel to support network and computer systems administration efforts as follows:

a. Be responsible for the O&M of networks, servers, and client workstations.

b. Install configure, maintain, and administer networks, network devices, client machines, and servers.

c. Implement and support application packages.

d. Procure and repair components necessary to maintain network and information technology systems.

e. Conduct systems analysis and summarize the data collected in a technical document written in a manner that is understood and usable by the decision makers.

f. Maintain system backups.

g. Recognize/Examine a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact and preserve evidence.

h. Apply instructions and pre-established guidelines to perform Cyber Security tasks within the computing environment (CE).

i. Provide end user Cyber Security support for computer environment systems, peripherals, and applications.

j. Support, monitor, test, and troubleshoot HW and SW Cyber Security problems pertaining to their CE.

k. Apply CE-specific Cyber Security program requirements to identify areas of weakness.

l. Apply appropriate CE access controls.

m. Install and operate the Network and computer systems in a test configuration manner that does not alter the program code or compromise security safeguards.

n. Conduct tests of Cyber Security safeguards for CE system in accordance with implementation plans and SOPs.

o. Apply established Cyber Security procedures and safeguards and comply with responsibilities assignment.

p. Develop and implement access control lists on switches and other network devices.

q. Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.

r. Implement applicable patches including IAVAs, IAVBs and IATAs for CE COTS.

s. Understand and implement technical vulnerability corrections (i.e., workarounds, mitigations and/or remediation)

t. Coordinate Certification and Accreditation activities with Information Security Officer/Manager.

u. Perform penetration tests and vulnerability assessments using EyeRetina vulnerability scanner, Defense Information Systems Agency (DISA) Gold Disk and Security Readiness Review (SRR) scripts as required.

v. Support Security Test & Evaluations or Validation Tests (Part of Certification and Accreditation Process).

w. Ensure compliance with Department of the Navy Application & Database Management System (DADMS) validation requirements for commercial of the shelf (COTS) and Government of the shelf (GOTS) SW products used in the CE. Request a Government-sponsored DADMS access account.

3.2.2.3 Cyber Security and Network and Computer Systems Support for Level I Computing Environments.

Level I Computing Environments are defined in DoD 8570.01-M. The Contractor shall assist the Government ISEO by providing appropriately certified personnel. The personnel shall support network, servers, client workstations and computer system O&M efforts as follows:

a. Design of systems architectures.

b. Design and document network architectures comprised of network topologies, network devices, client machines, and servers.

c. Investigate, recommend, implement, and support application packages.

d. Recommend procurement and repair of components necessary to maintain the network and information technology systems.

e. Conduct systems analysis and produce specific charts, graphs, databases, or other documentation that summarize the data collected in a manner that is understood and usable by the decision makers.

f. Recognize/Examine a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact and preserve evidence.

g. Apply instructions and pre-established guidelines to perform Cyber Security tasks within the computing environment (CE).

h. Provide end user Cyber Security support for computer environment systems, peripherals, and applications.

i. Support, monitor, test, and troubleshoot HW and SW Cyber Security problems pertaining to their CE.

j. Apply CE specific Cyber Security program requirements to identify areas of weakness.

k. Apply appropriate CE access controls.

l. Install and operate the Network and computer systems in a test configuration manner that does not alter the program code or compromise security safeguards.

m. Conduct tests of Cyber Security safeguards for CE system in accordance with implementation plans and SOPs.

n. Apply established IS security procedures and safeguards and comply with responsibilities assignment.

o. Develop and implement access control lists on switches and other network devices.

p. Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.

q. Implement applicable patches including IAVAs, IAVBs and IATAs for CE COTS.

r. Understand and implement technical vulnerability corrections (i.e., workarounds, mitigations and/or remediation)

s. Coordinate Certification and Accreditation activities with Information Security Officer/Manager.

t. Support Security Test & Evaluations or Validation Tests (Part of Certification and Accreditation Process).

3.2.2.4 Cyber Security and Network and Computer Systems Support Network Environments (Non-IAT).

The Contractor shall assist with network and computer systems efforts as follows.

a. Design of systems architectures.

b. Design and document network architectures comprised of network topologies, network devices, client machines, and servers.

c. Investigate, recommend, implement, and support application packages.

d. Recommend procurement and repair of components necessary to maintain the network and information technology systems.

e. Conduct systems analysis and produce specific charts, graphs, databases, or other documentation that summarize the data collected in a manner that is understood and usable by the decision makers.

f. Ensure that network device program activities are carried out for the network control devices (e.g., firewalls, routers, switches), IAW DOD Cyber Security policy and organization specific guidelines, including maintaining configuration of network control devices IAW Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs) and National Security Agency (NSA) security guidelines to protect the network control devices from unauthorized access.

g. Conduct quarterly tests on network(s) for changes and updates made to the network control devices to ensure integrity IAW the systems Configuration Management Plan.

3.2.2.5 IPT Support for SW Maintenance of Fielded Platform IT Training Systems.

The Contractor shall provide Integrated Product Team (IPT) support for operation, maintenance and repair of trainer Platform IT. Specific support may include but not be limited to:

a. Analyzing technical documentation and assist in preparing technical design approaches for training system modifications. The technical design approach shall provide alternative design approaches that will include trade-off analyses and identify technical risks.

b. Analyzing and assist in identifying facility requirements such as size of buildings, air conditioning, electrical power and grounding, raised flooring, etc. to satisfy training requirements.

c. Analyzing and assessing Engineering Change Proposals (ECP), Airframe Changes (AFC), Rapid Action Maintenance/Minor Engineering Changes (RAMECs), Technical Equipment Change Directives (TECDs), Training Equipment Change Requests (TECRs), and other requirement documents to determine the validity, feasibility, resource requirements, and any potential impact to training systems.

d. Providing support in developing engineering specifications detailing design, performance, testing, and provisions for the acceptance of the engineering changes.

e. Providing support in developing Engineering Specifications, SOWs and other documents required by NAWCTSD's policies and procedures on Technical Procurement Package Preparation and Processing.

f. Assisting in the review of training system Contractor's design approach, criteria, and design reports.

g. Recommending changes to the Government for training systems contract based on revisions to military training characteristics, changes to performance characteristics, or for pre-planned product improvements.

h. Identifying problems being encountered in HW and SW development and provide recommendations as to how to resolve these problems.

i. Assisting in reviewing the training system Contractor's proposed test criteria and subsequently perform examinations

j. Assisting the Government with acceptance testing. This can range from small modifications to full complex training system with motion platforms. Perform and document SW cold starts and other SW related system testing.

k. Analyzing potential requirements for modifications on training systems in the operational phase of the training system and provide recommendations to the Government. This involves extensive research and coordination, including direct contact with fleet activities, Government laboratories, and device/system users.

l. Assist in reviewing Contractor's data deliverable (CDRL items) and internal SW work products (e.g. System Engineering Plan, SW Development Plan, System and SW Requirements Specs, System and SW Design Descriptions, SW Test Plans/Procedures, and other Technical Reports).

m. Continuously monitoring and assessing performance and recommend appropriate action when Contractor delinquencies or deficiencies occur in the trainer.

n. Becoming familiar with the training system Contractor's SW activities and work products, in order to effectively monitor and assess the SW development effort.

o. Attend and contribute functional expertise in appropriate meetings.

p. Monitoring and evaluating SW metrics data for trends, deviations, and compliance.

q. Monitoring the requirements analysis, definition and allocation process and work products generated in the training system.

r. Monitoring the SW preliminary and detailed design process and related work products generated in the training system.

s. Monitoring the SW code and unit test process and work products generated in the training system. Review the training system Contractor's proposed test criteria and subsequently perform examinations and audit test results.

t. Monitoring and participating in the HW and SW Integration (HSI) process and work products generated in the training system.

u. Monitoring and participate in the SW Physical Configuration Audit.

v. Monitoring the SW configuration management process applied and work products generated in the training system.

w. Monitoring the SW quality assurance process applied, and work products generated in the training system.

x. Assisting in identifying problems being encountered in HW and SW development and provide recommendations as to how to resolve these problems.

y. Assisting in the analysis of potential HW and/or SW requirements for modifications on training systems in the operational phase of the training system. This involves extensive research and coordination, including direct contact with fleet activities, Government laboratories, and device/system users.

3.2.2.6 Documentation Development and Maintenance Support.

The Contractor shall assist the Government ISEO in:

a. Developing documentation updates for approved trainer system modification efforts.

b. Updating the content of training systems technical data affected by modification, including: Engineering documents; engineering drawings and associated lists; testing procedures; O&M manuals; instructor handbooks; SW user's handbooks; Commercial Off-the-Shelf (COTS) and vendor manuals; and diagrams, flowcharts, drawings, and other graphically-represented data.

c. Developing and maintaining quality control policies and procedures for trainer technical data changes and revisions, and update the Technical Data Package Quality Plan.

d. Supporting the development and maintenance of a relational database management application that is adaptable to rapid expansion, and provides status and cross-reference capability of the technical data.

e. Maintaining and providing physical and configuration control of documentation, data, and media in the technical library.

f. Converting documentation to portable electronic media. Updated and new documentation and drawings shall be produced using desktop publishing and drafting applications on computer systems provided.

3.2.2.7 Fabrication Support.

The Contractor shall assist with the building, fabrication, testing, evaluation, and operation of reduced and full-scale models, mock-ups, prototypes, and pre-production units. This includes support of fabrication and machining of trainer parts or equipment for fielded systems using traditional materials as well as new composite materials. This task is for support only and would be carried out using Government owned tools and Government purchased materials.

3.2.2.8 Configuration Management (CM) Support.

The Contractor shall assist the Government ISEO in applying engineering and analytical disciplines to identify, document, and verify the functional, performance, and physical characteristics of systems, to control changes and non-conformance and to track actual configurations of systems and platforms. This applies to Information System HW and SW items. Contractors shall provide CM support for HW and SW Documentation baselines as follows:

a. Provide support in developing and maintaining SW, HW, and technical data configuration management policies and procedures, and perform CM planning for SW, HW, and technical data. The Contractor shall maintain Configuration Management Plans, Configuration Status Accounting (CSA) and other databases.

b. Implement the configuration management procedures established in the Government ISEO's Configuration Management Plan for identification, evaluation, documentation and control of training system modifications.

c. Use Government-developed or owned commercial SW tools to implement automated/electronic change management, configuration control, and archive procedures for trainer system and other configuration items. This includes, but is not limited to, use of the NAWCTSD Training Information Electronic Resource System (TIERS).

d. Develop and maintain SW build procedures for each device. This includes all procedures required to edit, compile, assemble, build, and link the SW undergoing development or

modification. Archive the documented procedures and maintain the sources for each program revision.

e. Support trainer SW releases by preparing cold start SW kit and the Computer SW Product End Items for each device.

3.2.2.9 Interoperability Support/Fleet Synthetic Training (FST) Support.

The Contractor shall provide support to FST efforts. The Contractor shall perform the following work:

a. Provide technical support to Navy Warfare Development Command (NWDC, Navy Continuous Training Environment (NCTE) and Advance Distributed Virtual Training Environment (ADVTE) engineers to troubleshoot problems encountered with connectivity issues and new trainer capabilities.

b. Provide technical support to ensure successful integration and performance of the training device during actual FST events.

3.2.2.10 Supply and Provisioning Support.

The Government ISEO is responsible for decision-making pertaining to determining the supplies or services to be acquired by the Government. The Contractor shall support the Government ISEO in the procurement or requisition of equipment, parts, SW, and documentation related to trainer O&M of Platform IT or ISEO operations. This may include, but is not limited to, order processing, order tracking, inspection of goods received, and inventory management.

APPENDIX A

Appendix A provides the twenty (20) specific Labor Categories and their descriptions that will support the detailed requirements listed in paragraph 3.2 above.

#	SOW Appendix A	Labor Categories
1	A.1	Technical Writer III
2	A.2	Technical Writer II
3	A.3	Electronics Technician, Maintenance, Senior
4	A.4	Drafter/CAD Operator, Journey Level
5	A.5	Documentation Specialist
6	A.6	Software Engineer, Senior
7	A.7	Software Engineer, Journey Level
8	A.8	Software Engineer, Junior
9	A.9	System Administrator, Senior
10	A.10	System Administrator, Junior
11	A.11	Systems Analyst, Senior
12	A.12	Systems Analyst, Journey Level
13	A.13	Computer Scientist
14	A.14	Network Engineer
15	A.15	Engineer/Scientist, Senior
16	A.16	Engineer/Scientist, Journey Level
17	A.17	Engineer/Scientist, Junior
18	A.18	Order Clerk II
19	A.19	Information Assurance Analyst, Senior
20	A.20	Information Assurance Analyst

A.1 Technical Writer III, BLS SOC 27-3042

a. EDUCATION – Minimum of High School diploma or GED; Vocational training commensurate with Department of Labor functional description as follows: develops, writes, and edits material for reports, manuals, briefs, proposals, instruction books, catalogs, and related technical and administrative publications concerned with work methods and procedures, and installation, operation, and maintenance of machinery and other equipment.

b. EXPERIENCE – Minimum of five (5) years of experience in developing technical manuals, such as system design documents, configuration drawings, operation manuals, maintenance manuals, and training manuals.

A.2 Technical Writer II, BLS SOC 27-3042

a. EDUCATION – Minimum of High School diploma or GED; Vocational training commensurate with Department of Labor functional description as follows: develops, writes, and edits material for reports, manuals, briefs, proposals, instruction books, catalogs, and related technical and administrative publications concerned with work methods and procedures, and installation, operation, and maintenance of machinery and other equipment.

b. EXPERIENCE – Minimum of two (2) years of experience in developing technical manuals, such as system design documents, configuration drawings, operation manuals, maintenance manuals, and training manuals.

A.3 Electronics Technician, Maintenance, Senior, BLS SOC 17-3023

a. EDUCATION - At a minimum shall be a graduate of an accredited technical or computer school, with related vendor sponsored training classes. May substitute additional four (4) years of relevant work experience for the "graduate of an accredited technical or computer school" requirement.

b. EXPERIENCE - Minimum of seven (7) years relevant work experience in installation, troubleshooting, and maintenance of electronics equipment, large computers, minicomputers, or microprocessors, including those in a networked environment.

c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.4 Drafter/CAD Operator, Journey Level, BLS SOC 17-3012

a. EDUCATION – Minimum of High School diploma or GED.

b. EXPERIENCE - Minimum of five (5) years of relevant progressive work experience in drafting with a professional working knowledge of drafting methods, procedures, and techniques, and use of computer aided design (CAD).

A.5 Documentation Specialist, BLS SOC 43-9022

a. EDUCATION – Minimum of High School diploma or GED.

b. EXPERIENCE – Minimum of 2 years general clerical experience and experience with MS Office, including Excel, Access, Power Point, and Word.

A.6 Software Engineer, Senior, BLS SOC 15-1133

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.
b. EXPERIENCE - At least seven (7) years of practical experience in software development.
c. CERTIFICATIONS – Required - Minimum of an IAT-I certification in accordance SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.7 Software Engineer, Journey Level, BLS SOC 15-1133

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.
b. EXPERIENCE - At least three (3) years of practical experience in software development.
c. CERTIFICATIONS– Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.8 Software Engineer, Junior, BLS SOC 15-1133

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.
b. EXPERIENCE- Experience in software development.
c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.9 System Administrator, Senior, BLS SOC 15-1142

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer information systems, computer science, or a B.A. degree in Management Information Sciences. Eight (8) years of related work experience may be substituted for education requirement.
b. EXPERIENCE – Minimum of five (5) years of experience as a network and computer systems administrator.
c. CERTIFICATIONS - Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b).

A.10 System Administrator, Junior, BLS SOC 15-1142

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer information systems, computer science, or a B.A. degree in Management Information Sciences. Three (3) years of related work experience may be substituted for education requirement.
b. EXPERIENCE – Minimum of one (1) year of experience as a network and computer systems administrator.
c. CERTIFICATIONS - Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b).

A.11 Systems Analyst, Senior, BLS SOC 15-1121

a. EDUCATION – Minimum of M.S./M.A. degree in electronics engineering, electrical engineering, computer engineering, computer science, mathematics, or physics. A B.S./B.A. degree and an additional four (4) years of experience can be substituted for a M.S. or M.A. degree.
b. EXPERIENCE – A minimum of ten (10) years of experience in the design, integration, and test of systems.
c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.12 Systems Analyst, Journey Level, BLS SOC 15-1121

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer science, mathematics, or physics.
b. EXPERIENCE – A minimum of six (6) years of experience in the design, integration, and test of systems.
c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.13 Computer Scientist, BLS SOC 15-1132

a. EDUCATION – Minimum of B.S. in Computer Science.
b. EXPERIENCE – At least three (3) years of experience in the application of computer science principles to develop new software and computer hardware solutions.
c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.14 Network Engineer, BLS SOC 15-1143

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer science, computer information systems, or

mathematics. 8 yrs. of related work experience may be substituted for education requirement.

b. EXPERIENCE – Minimum of five (5) years of engineering or network/computer systems administrator experience with at least 1 year of Cyber Security experience.

c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b).

A.15 Engineer /Scientist, Senior (Hardware Engineer, Senior), BLS SOC 17-2061

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE - At least six (6) years of hardware design and integration experience.

c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.16 Engineer/Scientist, Journey Level (Hardware Engineer), BLS SOC 17-2061

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE - At least three (3) years of hardware design and integration experience.

c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.17 Engineer /Scientist, Junior (Hardware Engineer, Junior), BLS SOC 17-2061

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE – Experience in hardware design and integration.

c. CERTIFICATIONS – Minimum of an IAT-I certification in accordance with SOW Appendix C paragraph 2.0 (b) unless otherwise specified in Attachment J-5 Funded Level of Effort Spreadsheet.

A.18 Order Clerk II, BLS SOC 43-4151

a. EDUCATION - Minimum of High School Graduate or equivalent.

b. EXPERIENCE – Minimum of five (5) years of experience.

A.19 Information Assurance Analyst, Senior, BLS SOC 15-1122

a. EDUCATION - Minimum of B.S. or B.A. degree in Computer Science, Information Systems or a "Relevant Technical Discipline". An A.S. or A.A. degree and an additional three (3) years of experience can be substituted for degree requirement.

b. EXPERIENCE - At least seven (7) years of cyber security experience in secure network and system design, analysis, procedure/test generation, test execution and implementation of computer/network security mechanisms.

c. CERTIFICATIONS – Minimum of DOD Approved Baseline Certification as Information Assurance Technical (IAT) Level II in accordance with DOD 8570.01-M.

A.20 Information Assurance Analyst, BLS SOC 15-1122

a. EDUCATION - Minimum of B.S. or B.A. degree in Computer Science, Information Systems or a "Relevant Technical Discipline". An A.S. or A.A. degree and an additional three (3) years of experience can be substituted for degree requirement.

b. EXPERIENCE - At least four (4) years of cyber security experience in secure network and system design, analysis, procedure/test generation, test execution and implementation of computer/network security mechanisms.

c. CERTIFICATIONS – Minimum of DOD Approved Baseline Certification as Information Assurance Technical (IAT) Level I in accordance with DOD 8570.01-M.

APPENDIX B

Appendix B provides the estimate of Labor Mix. Based on workload trends and forecasts, the appendix represents the anticipated level of effort required to satisfy the immediate requirement of the Naval Air Warfare Center Training Systems Division. This appendix utilizes the labor categories as defined in this document. For evaluation purposes only, offerors will utilize this appendix as the labor mix, which will be evaluated in accordance with Section M of the solicitation.

PERIOD 1 (Base Year CSD, 10 months)

Program	Labor Categories	Hours Req	Total Hours
Whidbey Island			
EA-6B OMN			10320
PMA 205	Software Engineer, Journey Level	1600	
	Technical Writer II	1600	
	Documentation Specialist	1680	
	Computer Scientist	3360	
	System Administrator, Senior	1600	
	Electronics Technician, Maintenance, Senior	320	
	Journey Drafter/CAD Operator	160	
EP-3 P-3 P-8 Minor & Cyber Security Support			4464
CNAF AIRPAC	Information Assurance Analyst	3200	
	Software Engineer, Journey Level	1264	
EP-3 Whidbey			336
PMA 205	Software Engineer, Journey Level	336	
Jacksonville			
P-3			11200
PMA 205	Software Engineer, Senior	3200	
	Software Engineer, Journey Level	3200	
	Technical Writer III	1600	
	System Administrator, Senior	1600	
	Order Clerk II	1600	
Cyber Security P-3 & P-8 Support			3200
CNAF AIRLANT	Information Assurance Analyst, Senior	1600	
	Information Assurance Analyst	1600	
Oceana			
LSO			1600

PMA 205	Software Engineer, Senior	1600	
Norfolk			
E-2			20613
PMA 205	Software Engineer, Senior	9333	
	Electronics Technician, Maintenance, Senior	3200	
	Documentation Specialist	80	
	System Administrator, Senior	6400	
	Technical Writer II	1600	
Cyber Security Support E-2			1600
CNAF AIRLANT	Information Assurance Analyst	1600	
MH-53			5067
PMA 205	Software Engineer, Senior	1867	
	Electronics Technician, Maintenance, Senior	1600	
	Documentation Specialist	1600	
Cherry Point			
AV-8B			21784
PMA 205	Software Engineer, Senior	3200	
	Software Engineer, Journey Level	6400	
	Software Engineer, Junior	1600	
	System Administrator, Junior	1600	
	System Administrator, Senior	1067	
	Electronics Technician, Maintenance, Senior	1600	
	Documentation Specialist	3117	
	Computer Scientist	1600	
	Engineer/Scientist, Junior	1600	
KC-130			3465
PMA 205	Software Engineer, Journey Level	1600	
	Technical Writer II	800	
	System Administrator, Senior	265	
	Engineer/Scientist, Senior	800	
KC-130 & F-5			5065
RESFOR	Software Engineer, Journey Level	1600	
	Technical Writer II	800	
	System Administrator, Senior	265	
	Engineer/Scientist, Senior	800	
	Software Engineer, Journey Level	1600	
New River			
Cyber Security Support			1600
CNAF AIRLANT	Information Assurance Analyst, Senior	1600	

Yuma			
AV-8B			1600
PMA 205	Electronics Technician, Maintenance, Senior	1600	
North Island			
MH-60R			3600
PMA 205	Software Engineer, Journey Level	400	
	Systems Analyst, Senior	1600	
	Systems Analyst, Journey Level	800	
	Documentation Specialist	800	
MH-60S			2800
PMA 205	Software Engineer, Journey Level	1200	
	Systems Analyst, Journey Level	800	
	Documentation Specialist	800	
San Diego			
Cyber Security Support			4800
CNAF AIRPAC	Information Assurance Analyst, Senior	1600	
	Information Assurance Analyst	1600	
	Information Assurance Analyst, Senior	1600	
Miramar			
ADVTE			1600
CNAF AIRPAC	Network Engineer	1600	
Camp Pendleton			
H-1			3200
PMA 205	Software Engineer, Junior	1600	
	Documentation Specialist	1600	
Pensacola			
CNATRA			3200
PMA 205	Software Engineer, Senior	1600	
	Engineer/Scientist Journey Level	1600	
ATC			9600
PMA 205	Electronics Technician, Maintenance, Senior	1600	
	Documentation Specialist	6400	
	Software Engineer, Junior	1600	
Kingsville			
CNATRA			1600
PMA 205	Software Engineer, Junior	1600	
Newport			

LCS			4800
SWOS	Electronics Technician, Maintenance, Senior	4800	
Atsugi & Iwakuni Japan			
At. H-60 & Iw. F-18/USMC			3200
CNAF AIRPAC	System Administrator, Senior	3200	
TOTALS		**130314**	**130314**

PERIOD 2 (Option, 12 months)

Program	Labor Categories	Hours Req	Total Hours
Whidbey Island			
EA-6B OMN			12384
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	1920	
	Documentation Specialist	2016	
	Computer Scientist	4032	
	System Administrator, Senior	1920	
	Electronics Technician, Maintenance, Senior	384	
	Journey Drafter/CAD Operator	192	
EP-3 P-3 P-8 Minor & Cyber Security Support			5357
CNAF AIRPAC	Information Assurance Analyst	3840	
	Software Engineer, Journey Level	1517	
EP-3 Whidbey			403
PMA 205	Software Engineer, Journey Level	403	
Jacksonville			
P-3			13440
PMA 205	Software Engineer, Senior	3840	
	Software Engineer, Journey Level	3840	
	Technical Writer III	1920	
	System Administrator, Senior	1920	
	Order Clerk II	1920	
Cyber Security P-3 & P-8 Support			3840
CNAF AIRLANT	Information Assurance Analyst, Senior	1920	
	Information Assurance Analyst	1920	
Oceana			
LSO			1920
PMA 205	Software Engineer, Senior	1920	
Norfolk			
E-2			24736
PMA 205	Software Engineer, Senior	11200	
	Electronics Technician, Maintenance, Senior	3840	
	Documentation Specialist	96	
	System Administrator, Senior	7680	

	Technical Writer II	1920	
Cyber Security Support E-2			1920
CNAF AIRLANT	Information Assurance Analyst	1920	
MH-53			6080
PMA 205	Software Engineer, Senior	2240	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	1920	
Cherry Point			
AV-8B			26140
PMA 205	Software Engineer, Senior	3840	
	Software Engineer, Journey Level	7680	
	Software Engineer, Junior	1920	
	System Administrator, Junior	1920	
	System Administrator, Senior	1280	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	3740	
	Computer Scientist	1920	
	Engineer/Scientist, Junior	1920	
KC-130			4158
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
KC-130 & F-5			6078
RESFOR	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
	Software Engineer, Journey Level	1920	
New River			
Cyber Security Support			1920
CNAF AIRLANT	Information Assurance Analyst, Senior	1920	
Yuma			1920
AV-8B			
PMA 205	Electronics Technician, Maintenance, Senior	1920	

North Island			
MH-60R			4320
PMA 205	Software Engineer, Journey Level	480	
	Systems Analyst, Senior	1920	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
MH-60S			3360
PMA 205	Software Engineer, Journey Level	1440	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
San Diego			
Cyber Security Support			5760
CNAF AIRPAC	Information Assurance Analyst, Senior	1920	
	Information Assurance Analyst	1920	
	Information Assurance Analyst, Senior	1920	
Miramar			
ADVTE			1920
CNAF AIRPAC	Network Engineer	1920	
Camp Pendleton			
H-1			3840
PMA 205	Software Engineer, Junior	1920	
	Documentation Specialist	1920	
Pensacola			
CNATRA			3840
PMA 205	Software Engineer, Senior	1920	
	Engineer/Scientist Journey Level	1920	
ATC			11520
PMA 205	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	7680	
	Software Engineer, Junior	1920	
Kingsville			
CNATRA			1920
PMA 205	Software Engineer, Junior	1920	
Newport			
LCS			5760
SWOS	Electronics Technician, Maintenance, Senior	5760	

Atsugi & Iwakuni Japan			
At. H-60 & Iw. F-18/USMC			3840
CNAF AIRPAC	System Administrator, Senior	3840	
TOTALS		**156376**	**156376**

PERIOD 3 (Option, 12 months)

Program	Labor Categories	Hours Req	Total Hours
Whidbey Island			
EA-6B OMN			12384
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	1920	
	Documentation Specialist	2016	
	Computer Scientist	4032	
	System Administrator, Senior	1920	
	Electronics Technician, Maintenance, Senior	384	
	Journey Drafter/CAD Operator	192	
EP-3 P-3 P-8 Minor & Cyber Security Support			5357
CNAF AIRPAC	Information Assurance Analyst	3840	
	Software Engineer, Journey Level	1517	
EP-3 Whidbey			403
PMA 205	Software Engineer, Journey Level	403	
Jacksonville			
P-3			13440
PMA 205	Software Engineer, Senior	3840	
	Software Engineer, Journey Level	3840	
	Technical Writer III	1920	
	System Administrator, Senior	1920	
	Order Clerk II	1920	
Cyber Security P-3 & P-8 Support			3840
CNAF AIRLANT	Information Assurance Analyst, Senior	1920	
	Information Assurance Analyst	1920	
Oceana			
LSO			1920
PMA 205	Software Engineer, Senior	1920	
Norfolk			
E-2			24736
PMA 205	Software Engineer, Senior	11200	
	Electronics Technician, Maintenance, Senior	3840	
	Documentation Specialist	96	
	System Administrator, Senior	7680	

	Technical Writer II	1920	
Cyber Security Support E-2			1920
CNAF AIRLANT	Information Assurance Analyst	1920	
MH-53			6080
PMA 205	Software Engineer, Senior	2240	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	1920	
Cherry Point			
AV-8B			26140
PMA 205	Software Engineer, Senior	3840	
	Software Engineer, Journey Level	7680	
	Software Engineer, Junior	1920	
	System Administrator, Junior	1920	
	System Administrator, Senior	1280	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	3740	
	Computer Scientist	1920	
	Engineer/Scientist, Junior	1920	
KC-130			4158
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
KC-130 & F-5			6078
RESFOR	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
	Software Engineer, Journey Level	1920	
New River			
Cyber Security Support			1920
CNAF AIRLANT	Information Assurance Analyst, Senior	1920	
Yuma			
AV-8B			1920
PMA 205	Electronics Technician, Maintenance, Senior	1920	

North Island			
MH-60R			4320
PMA 205	Software Engineer, Journey Level	480	
	Systems Analyst, Senior	1920	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
MH-60S			3360
PMA 205	Software Engineer, Journey Level	1440	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
San Diego			
Cyber Security Support			5760
CNAF AIRPAC	Information Assurance Analyst, Senior	1920	
	Information Assurance Analyst	1920	
	Information Assurance Analyst, Senior	1920	
Miramar			
ADVTE			1920
CNAF AIRPAC	Network Engineer	1920	
Camp Pendleton			
H-1			3840
PMA 205	Software Engineer, Junior	1920	
	Documentation Specialist	1920	
Pensacola			
CNATRA			3840
PMA 205	Software Engineer, Senior	1920	
	Engineer/Scientist Journey Level	1920	
ATC			11520
PMA 205	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	7680	
	Software Engineer, Junior	1920	
Kingsville			
CNATRA			1920
PMA 205	Software Engineer, Junior	1920	
Newport			
LCS			5760
SWOS	Electronics Technician, Maintenance,	5760	

	Senior		
Atsugi & Iwakuni Japan			
At. H-60 & Iw. F-18/USMC			3840
CNAF AIRPAC	System Administrator, Senior	3840	
TOTALS		**156376**	**156376**

PERIOD 4 (Option, 12 months)

Program	Labor Categories	Hours Req	Total Hours
Whidbey Island			
EA-6B OMN			12384
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	1920	
	Documentation Specialist	2016	
	Computer Scientist	4032	
	System Administrator, Senior	1920	
	Electronics Technician, Maintenance, Senior	384	
	Journey Drafter/CAD Operator	192	
EP-3 P-3 P-8 Minor & Cyber Security Support			5357
CNAF AIRPAC	Information Assurance Analyst	3840	
	Software Engineer, Journey Level	1517	
EP-3 Whidbey			403
PMA 205	Software Engineer, Journey Level	403	
Jacksonville			
P-3			*13440*
PMA 205	Software Engineer, Senior	*3840*	
	Software Engineer, Journey Level	*3840*	
	Technical Writer III	*1920*	
	System Administrator, Senior	*1920*	
	Order Clerk II	*1920*	
Cyber Security P-3 & P-8 Support			*3840*
CNAF AIRLANT	Information Assurance Analyst, Senior	*1920*	
	Information Assurance Analyst	*1920*	
Oceana			
LSO			*1920*
PMA 205	Software Engineer, Senior	*1920*	
Norfolk			
E-2			24736
PMA 205	Software Engineer, Senior	11200	
	Electronics Technician, Maintenance, Senior	3840	
	Documentation Specialist	96	

	System Administrator, Senior	7680	
	Technical Writer II	1920	
Cyber Security Support E-2			1920
CNAF AIRLANT	Information Assurance Analyst	1920	
MH-53			6080
PMA 205	Software Engineer, Senior	2240	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	1920	
Cherry Point			
AV-8B			26140
PMA 205	Software Engineer, Senior	3840	
	Software Engineer, Journey Level	7680	
	Software Engineer, Junior	1920	
	System Administrator, Junior	1920	
	System Administrator, Senior	1280	
	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	3740	
	Computer Scientist	1920	
	Engineer/Scientist, Junior	1920	
KC-130			4158
PMA 205	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
KC-130 & F-5			6078
RESFOR	Software Engineer, Journey Level	1920	
	Technical Writer II	960	
	System Administrator, Senior	318	
	Engineer/Scientist, Senior	960	
	Software Engineer, Journey Level	1920	
New River			
Cyber Security Support			1920
CNAF AIRLANT	Information Assurance Analyst, Senior	1920	
Yuma			
AV-8B			1920
PMA 205	Electronics Technician, Maintenance, Senior	1920	

North Island			
MH-60R			4320
PMA 205	Software Engineer, Journey Level	480	
	Systems Analyst, Senior	1920	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
MH-60S			3360
PMA 205	Software Engineer, Journey Level	1440	
	Systems Analyst, Journey Level	960	
	Documentation Specialist	960	
San Diego			
Cyber Security Support			5760
CNAF AIRPAC	Information Assurance Analyst, Senior	1920	
	Information Assurance Analyst	1920	
	Information Assurance Analyst, Senior	1920	
Miramar			
ADVTE			1920
CNAF AIRPAC	Network Engineer	1920	
Camp Pendleton			
H-1			3840
PMA 205	Software Engineer, Junior	1920	
	Documentation Specialist	1920	
Pensacola			
CNATRA			3840
PMA 205	Software Engineer, Senior	1920	
	Engineer/Scientist Journey Level	1920	
ATC			11520
PMA 205	Electronics Technician, Maintenance, Senior	1920	
	Documentation Specialist	7680	
	Software Engineer, Junior	1920	
Kingsville			
CNATRA			1920
PMA 205	Software Engineer, Junior	1920	
Newport			
LCS			5760
SWOS	Electronics Technician, Maintenance,	5760	

	Senior		
Atsugi & Iwakuni Japan			
At. H-60 & Iw. F-18/USMC			3840
CNAF AIRPAC	System Administrator, Senior	3840	
TOTALS		**156376**	**156376**

APPENDIX C

Appendix C provides the NAWCTSD requirements for Physical Security, Operational Security and for Cyber Security.

1.0 Security Requirements.
The Contractor shall safeguard all classified information and meet all Security and Cyber Security requirements identified in the DD Form 254. The Contractor shall enforce these safeguards throughout the life of the contract including the transport and delivery phases. Most of the position/labor category equivalents require a Secret Security clearance at a minimum. Some positions/ labor categories (approximately 5% of all position/labor category equivalents) require a Top Secret Security clearance that personnel shall attain prior to reporting on-site for work.

Positions supporting the EP-3 and E-2C training systems will perform support functions in a TS/SCI environment. The Contractor shall have a Department of Defense (DoD) Top Secret clearance with Director, Central Intelligence Directorate (DCID) 6/4 eligibility for SCI to fulfill the requirements specified in the contract. A Top Secret Facility Clearance is required.

The Contractor shall consider all EP-3 and E-2C unclassified documentation provided to or generated by the Contractor to be program sensitive and shall strictly control all information. Secondary distribution of program documentation provided to the Contractor is authorized only with written approval from both the originating activity, and the platform Program Office or PMA-205. The Contractor shall not publicly release any unclassified documentation without written approval from the COR. The Contractor shall provide internal distribution of unclassified documents only to those personnel with a need-to-know. No one shall release documentation related to the platform to any foreign nationals. At the completion of the contract, the Contractor shall destroy all documentation not required by the Contractor in accordance with the Contractor's facility security guidelines.

The Contractor shall control all classified documents, SW, or HW received, or generated as part of this contract in accordance with current National Industrial Security Program (NISP) guidelines.

1.1 Personnel Security - Background Check (Physical Access to & Working on DoD Installations).
The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. Contractor personnel require a National Agency Check with Inquiries (NACI) or equivalent national security clearance (e.g. National Agency Check with Local Agency Checks including Credit Check (NACLC)) for permanent issuance of the credential. The Government may issue the credential upon favorable return of the FBI fingerprint check, pending final favorable completion of the NACI/equivalent, based on a commander/director risk management decision. An individual holding a valid national security clearance shall not require an additional submission of the NACI/equivalent. The Government limits access to restricted areas, controlled unclassified information (sensitive information), or Government equipment for Contractor

personnel to those individuals who are determined trustworthy as a result of the favorable completion of a NACI/equivalent or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, the appropriate DoD Agency may conduct a NACI/equivalent prior to permitting access. The contractor shall use the Standard Form 85P (Questionnaire for Public Trust Positions) in order to obtain the CAC *and* access to controlled unclassified information. Contractors shall submit the Standard Form 85P to the Government Contracting Agency for processing.

2.0 Cyber Security (CS).

The Contractor shall support the Government with maintaining data integrity and training device Authorization-to-Operate (ATO) or Platform Information Technology (PIT) Risk Approval (PRA) of all devices located at all sites in this contract. The Contractor shall:

a. Maintain trainer CS programs identified through CS architecture requirements, objectives, and policies; CS personnel; and CS processes and procedures. This includes the maintenance and performance of the tasks identified by security controls listed in Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, and National Institute of Standards and Technology Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, current edition, and Department of Defense Instruction (DoDI)8501.01, Cybersecurity, DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), and the Authorizing Official (AO) Authorization-To-Operate (ATO) for systems with Security Objectives of; Confidentiality (Impact Value of; High, Moderate or Low), Integrity (Impact Value of; Moderate or Low) and Availability (Impact Value of; Moderate or Low).

b. Provide certified Cybersecurity Technical personnel to perform Cybersecurity duties as required in DoD 8570.01-M/Appendix 3, paragraph AP3.1 to 3.3 and SECNAV M-5239.2.

c. Assist and support the site COR with the implementation of the Information Assurance Vulnerability Management Program (IAVMP); Computer Tasking Orders (CTOs) or Directives on trainers. Implement/install applicable Government-directed and Vendor patches including: Cyber Security Vulnerability Advisories for the trainer operating system(s) and SW applications. Assist and support the respective COR in vulnerability management updates. The COR will provide lists of required updates.

d. Ensure site CS and security procedures are followed IAW with configuration management policies and practices.

e. Support security control assessments as part of the Authorization Process.

f. Implement Government ISEO's directed technical vulnerability corrections.

g. Perform and record the periodic vulnerability scanning and tasking specified by the Maintenance Requirement Cards (MRC) on applicable HW at the sites assigned as requested by the COR.

h. As required, provide assistance to Information System Security Officers (ISSO) and the Government ISEO in support of the Vulnerability Remediation Asset Manager (VRAM), the Marine Corps Accreditation Support Tool (MCAST) and the enterprise Mission Assurance Support Service (eMASS) for training systems.

i. Implement and enforce upon Contractor workforce Department of the Navy (DON) systems account access and password policy IAW Secretary of the Navy (SECNAV) Manual M-5239.1 series.

j. Ensure the administration of privileged user accounts IAW system role-based access schemes as per site operating procedures and COR authorization. Assist the COR in maintaining accounts currency to ensure that individual accounts designated as inactive, suspended, or terminated are promptly deactivated and associated passwords are disabled and removed.

k. Ensure system audit logs are reviewed In Accordance With (IAW) MRC and any security violations are reported to the COR. Ensure audit log records are backed up and maintained IAW SP 800-53 controls.

l. Perform data backup as required by the MRC.

m. Perform Government ISEO-directed antivirus SW updates and virus scanning IAW SP 800-53, the security authorization package, and/or as required by the MRC.

n. Assist Government ISEO in the assessment of trainer CS posture and configuration management by providing the periodic vulnerability scan results, reporting CS patch implementation status, and verifying trainer SW configurations. Perform Host Based Security Systems (HBSS) tasking IAW SP 800-53, the security authorization package, and/or as required by the MRC.

o. Ensure all media and data storage is properly marked and labeled per policy and guidance documents (i.e., SECNAV M-5510.36 series).

p. Ensure that network device program activities are carried out for the network control devices (e.g., firewalls, routers, switches), IAW DOD policy and organization specific guidelines, including maintaining configuration of network control devices IAW Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs) and National Security Agency (NSA) security guidelines to protect the network control devices from unauthorized access.

q. Conduct quarterly tests on network(s) for changes and updates made to the network control devices to ensure integrity IAW the systems Configuration Management Plan (may be specified via a MRC).

r. Ensure all communications and transmissions of sensitive CS related information be carried out in a secure manner and IAW DoD and Navy approved means and process.

s. Ensure Contractor personnel receive initial and annual CS awareness training. All CS training shall be documented and available for COR review at any time. Site specific requirements are provided in site specific Appendices.

3.0 Security for Classified Programs.

The Contractor shall safeguard classified information and meet the security requirements identified in the DD Form 254. The Contractor shall enforce these safeguards throughout the life of the contract including the transport and delivery phases.

4.0 Operations Security (OPSEC).

The Contractor shall provide OPSEC protection for classified information and sensitive information. Security policy, procedures, and requirements for classified information are provided in paragraph 1.0 above. The Contractor shall enforce these safeguards throughout the life of the contract including the development, delivery, support phases, the disposition, and storage of classified and controlled unclassified information at contract completion. The Contractor shall prepare the OPSEC Plan IAW CDRL B003 Contractor's Operational Security Plan.

5.0 Personnel Security - Background Check (Physical Access to and Working on DoD Installations).

The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to DoD installations, facilities, buildings, controlled spaces, and access to U.S. Government information systems. A National Agency Check with Local Agency Checks including Credit Check (NACLC) will be required for permanent issuance of the credential. There shall be no additional NACLC submission for an individual holding a valid national security clearance. The Government may issue the credential upon favorable return of the Federal Bureau of Investigations (FBI) fingerprint check, pending final favorable completion of the NACLC. Contractors with clearances shall contact the NAWCTSD Security Office to initiate the CAC issuance process.

5.1 Personnel Security - Background Checks.

Contractor personnel working at Government sites and in the Contractor's own facilities supporting Government work shall undergo the company internal vetting process prior to gaining access to U.S. Government controlled unclassified information, or performing Government-related sensitive duties. Contractor personnel shall undergo the company internal vetting process prior to gaining access to U.S. Government controlled unclassified information. To comply with immigration law, the Contractor shall use the Employment Eligibility Verification Program (E-Verify) IAW FAR 52.222-54.

5.2 Personnel Security - Reporting of Adverse or Derogatory Information related to Contractors.

The Contractor shall report to the NAWCTSD Security Office adverse or derogatory information pertaining to on-site personnel (when applicable) or Contractor personnel in direct support of this contract. Information reported to the Government Contracting Agency shall be integrated and reported in Contractor Performance Assessment Reporting System (CPARS) on Contractor performance of Personnel Security (PERSEC) related aspects of Contractor performance.

a. Adverse or derogatory information reporting of Contractor personnel. Example: Domestic violence arrest, or other violent or sexual crime arrest or self-report.
b. When Contractor personnel receive a revocation of an Interim or denial for the issuance of a CAC until final adjudication
c. When a denial or suspension of clearance occurs for a Contractor employee
d. When Contractor employee receives a final denial of eligibility for a security clearance.

5.3 Cyber Security and Personnel Security Requirements for Accessing Government Information Technology (IT) Systems - Credentialing Standards.

The Contractor shall comply with the Cyber Security and personnel security requirements for accessing U.S. Government IT systems specified in the contract. Contractors requiring access to U.S. Government IT systems will be subject to a background check. The Contractor shall review and become familiar with the credentialing standards presented in OPM Memorandum for Issuing Personal Identity Verification Cards to use as an aid in their employee selection process. The NAWCTSD Security Office will apply the credentialing standards and execute the credentialing process for individual contractors.

5.4 Government-Issued Personal Identification Credentials.

The Contractor and Subcontractor(s) (when applicable) shall account for all forms of U.S Government-provided identification credentials (CAC or U.S. Government-issued identification badges) issued to the Contractor (or their employees in connection with performance) under the contract. The Contractor shall return such identification credentials to the issuing agency at the earliest of the circumstances listed below, unless otherwise determined by the U.S. Government. The Contracting Officer may delay final payment under the contract, if the Contractor or Subcontractor fails to comply with these requirements.

a. When no longer needed for contract performance.
b. Upon completion of the Contractor employee's employment.
c. Upon contract completion or termination.

5.5 Contractor "Out-processing" Policy.

The Contractor and Subcontractor(s) (when applicable) shall have in place (established and enforced) an "out-processing" policy for employees that leave the company, including suspension of account access, return of all PCs, laptops, smartphones, and other electronic devices (Government-furnished IT equipment and Contractor-issued IT equipment) that contain U.S. Government Controlled Unclassified Information. The Contractor shall also ensure that out-processed employees receive debriefings on the need to maintain confidentiality of U.S. Government Controlled Unclassified Information.

5.6 Unclassified Contractor-Owned Network Security - Safeguarding of Unclassified Controlled Technical Information.

The safeguarding of Controlled Unclassified Technical Information applies to Prime Contractors and their Subcontractors for information resident on or transiting through Contractor unclassified information systems. The Contractor shall provide security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure. The Contractor shall take means (defense-in-depth measures) necessary

to protect the confidentiality, integrity, and availability of Government controlled unclassified information. The Contractor shall manage and maintain contractor-owned unclassified IT network assets (including computer assets used for Contractor Teleworkers) used to process U.S. Government controlled unclassified information (sensitive information) IAW FAR 252.204-7012, The Contractor shall prevent U.S. Government controlled unclassified information from being placed or stored on peer-to-peer applications or social media applications on Contractor owned networks, including IT assets provided to Contractors in a Teleworker status. The Contractor shall manage and control networks (which contain U.S. Government controlled unclassified information) serving in a Continuity of Operations (COOP) capacity to meet the same personnel and security requirements identified in this SOW.

Table 1 -- Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800-53).

Access Control AC-2 AC-3(4) AC-4 AC-6 AC-7 AC-11(1) AC-17(2) AC-18(1) AC-19 AC-20(1) AC-20(2) AC-22	Audit & Accountability AU-2 AU-3 AU-6(1) AU-7 AU-8 AU-9	Identification and Authentication IA-2 IA-4 IA-5(1)	Media Protection MP-4 MP-6	System & Comm Protection SC-2 SC-4 SC-7 SC-8(1) SC-13 SC-15 SC-28
	Configuration Management CM-2 CM-6 CM-7 CM-8	Incident Response IR-2 IR-4 IR-5 IR-6	Physical and Environmental Protection PE-2 PE-3 PE-5	
		Maintenance MA-4(6) MA-5 MA-6	Program Management PM-10	System & Information Integrity SI-2 SI-3 SI-4
Awareness & Training AT-2	Contingency Planning CP-9		Risk Assessment RA-5	

Legend:

AC: Access Control
AT: Awareness and Training
AU: Auditing and Accountability
CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response
MA: Maintenance
MP: Media Protection
PE: Physical & Environmental Protection
PM: Program Management
RA: Risk Assessment
SC: System & Communications Protection
SI: System & Information Integrity

5.7 Cyber Incident and Compromise Reporting.

The contractor shall report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems. The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (*http://dibnet.dod.mil/*) within 72 hours of discovery of a cyber-incident using the reporting criteria and requirements set forth IAW FAR 252.204-7012. The contractor shall also provide the report to the NAWCTSD Contracting Officer, NAWCTSD Security Manager, and the NAWCTSD Cyber Security Manager.

5.8 Reportable Cyber Incidents.

Reportable cyber incidents include the following:

a. A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of unclassified controlled technical information resident on or transiting through Contractor's, or its Subcontractors', unclassified information systems.
b. Activities that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

5.9 Access to restricted areas, controlled unclassified information (sensitive information), or Government Information Technology.

Access to restricted areas, controlled unclassified information (sensitive information), or Government Information Technology by Contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NACLC or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NACLC shall be conducted and favorably reviewed by the DoD component, agency, or activity prior to permitting such access.

5.10 Contractor access to controlled unclassified information

For Contractor personnel performing sensitive duties including access to controlled unclassified information, but do not have a clearance to access classified information, the Contractor shall use the Standard Form 86 (Questionnaire for National Security Positions) in order to obtain the CAC. The Contractor shall submit the Standard Form 86 to the NAWCTSD Security Office for processing. Contractors shall contact the NAWCTSD Security Office to initiate the CAC issuance process.

5.11 E-Verify Program

E-Verify is a free program that allows employers electronically to verify the employment eligibility of all newly hired U.S. citizen and non-citizen employees. E-Verify allows U.S. employers to verify name, DOB, SSN, along with immigration information for non-citizens and compare against Federal databases in order to verify the employment eligibility of all new hires. The Contractor can register on-line at https://www.vis-dhs.com/employerregistration/, which provides instructions for completing the Memorandum of Understanding (MOU) required for

official registration for the program. Additional information about the program can be found at the E-Verify website at www.dhs.gov/E-Verify.

5.12 International Traffic and Arms Regulation (ITAR)

The Contractor shall ensure that foreign persons, as defined under section 120.16 of the International Traffic and Arms Regulation (ITAR) (22 CFR, Parts 120 – 130), are not given access to U.S. Government controlled unclassified information, sensitive information, defense articles, defense services, or technical data, as defined in the ITAR, Part 120 without proper issuance of an export license from the U.S. Government authority

5.13 Contractor actions to support DoD damage assessment

In response to the reported cyber incident, the Contractor shall:

a. Conduct further review of its unclassified network for evidence of compromise resulting from a cyber-incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise and other information systems on the network that were accessed as a result of the compromise;
b. Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and
c. Preserve and protect images of known affected information systems and all relevant monitoring and packet capture data for no less than 90 days from the cyber incident to allow DoD to request information or decline interest.

5.14 DoD damage assessment activities

If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report provide all of the damage assessment information gathered in accordance with FAR 252.204-7012. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

5.15 Protection of reported information.

Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with FAR 252.204-7012.

5.16 Information Security Requirements for Protection of Unclassified DoD Information On Non-DoD Systems

The Contractor shall safeguard unclassified DoD information stored on non-DoD information systems to prevent the loss, misuse, and unauthorized access to or modification of this information. Protection of unclassified DoD information not approved for public release on non-DoD Information Systems will be protected IAW DoDI 8582.01, Security of Unclassified DoD Information on non-DoD Information Systems. The Contractor shall:

a. Not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
b. Protect information by no less than one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
c. Sanitize media (e.g., overwrite) before external release or disposal.
d. Encrypt the information that has been identified as Controlled Unclassified Information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media, compact disks, using the best available encryption technology.
e. Limit information transfer to Subcontractors or teaming partners with a need to know and a commitment to the same level of protection.
f. Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS).
g. Encrypt organizational wireless connections and use encrypted wireless connection, where available, when traveling. When encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using no less than application-provided password protection level encryption.
h. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
i. Not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).
j. Provide protection against computer network intrusions and data exfiltration, including no less than the following:
    (1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
    (2) Monitoring and control of inbound and outbound network traffic (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as

firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(3) Prompt application of security-relevant SW patches, service packs, and hot fixes.

k. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., critical program information, Personally Identifiable Information (PII), export controlled information) IAW the requirements of the contract.

5.17 Critical Program Information (CPI)

The Contractor shall participate with the Government in the development of a Program Protection Plan (PPP), to include the identification of system related Critical Program Information (CPI), Critical Components (CC), and Controlled Unclassified Information (CUI).

The Contractor will participate with the Government in recommending protection strategies/countermeasures needed to safeguard CPI, CC, and CUI throughout the acquisition process at all locations from development to fielded systems.

The Contractor will provide a summary of protection of CPI, CC, and CUI to be presented at all program management and technical reviews. Protection efforts shall be reviewed in detail at key technical reviews (e.g., System Requirements Review [SRR], Preliminary Design Review [PDR], and Critical Design Review [CDR]).

The Contractor shall identify candidate CPI and Resident CPI (formerly called Critical Technology) which requires protection IAW DoDI 5200.39. The CPI identified shall be approved by the USG Program Manager. The CPI identification shall include a review of the system, unique integration, support equipment and the Non-Resident design/process/material aspects of the program. All identified CPI shall be protected with appropriate countermeasures.

The Contractor shall develop a Program Protection Implementation Plan (PPIP) to include all requirements outlined in the Government provided PPP. The PPIP shall be used as a focal point for the Contractor's Program Security efforts. The PPIP is derived from the PPP and should not restate what is written in the PPP but rather address specifically how the Contractor will implement Program Protection. The Contractor shall plan for and implement countermeasures which mitigate foreign intelligence collection, technology exploitation, supply chain threats, and system vulnerabilities relative to the protection of CPI, CC, and CUI.

2.2.14.3.20 The Contractor shall comply with DFARS 252.204-7012 SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013).

Protection of unclassified DoD information not approved for public release on non-DoD Information Systems will be protected IAW DoDI 8582.01, Security of Unclassified DoD Information on non-DoD Information Systems, Enclosure 3, and the Program's Security Classification Guide. The Contractor shall comply with DoDM 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI), Enclosures 3 & 4, for identification, protection and training requirements of CUI. The Contractor shall be

responsible for training their personnel and accomplishment of the out-processing procedures identified in DoDM 5200.01, Volume 4, Enclosure 4. The Contractor shall comply with DoD 5400.7-R, DoD Freedom of Information Act (FOIA) Program requirements

The Contractor shall ensure each Contractor/ Sub-Contractor employee supporting this contract completes Contractor developed and conducted Program Protection awareness training in Contractor format; (a) prior to performing any contract work, and (b) completes annual refresher course training throughout the period of performance. This training is specific to the protection of CPI, CC, and CUI and tailored to each facility handling, storing, processing CPI, CC, and CUI.

Additional inspections consisting of a review of Contractor/Sub-Contractor implementation of Government furnished Program Protection Plans may be required. This is above and beyond Defense Security Service inspections. The purpose of the inspection is to ensure CPI, CC, and CUI are protected as required by the PPP when not covered under NISPOM.
The Contractor will notify the Government Program Office of security incidents involving loss, compromise, or suspected compromise of CPI. CPI involved in the incident should be specifically identified in inquiry and investigation reports. Classify IAW program security classification guidance.

5.18 Contractor Counterfeit Electronic Part Detection and Avoidance System, in solicitations and contracts when procuring:

(1) Electronic parts;
(2) End items, components, parts, or assemblies containing electronic parts; or
(3) Services where the Contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service.
[SOWxxx1] The Contractor shall develop and update mission criticality analysis(-es), vulnerability assessment(s), risk assessments(s), and identification and counter measurement implementation(s) for Mission-Critical Functions, the failure of which would result in either Level I (Catastrophic) or Level II (Critical) compromise of mission capability.
[SOWxxx2] Adapting the MIL-STD-882 (System Safety) (https://assist.dla.mil) definitions of criticality to mission criticality, the Contractor shall define the following criticality levels:
• Level I (Catastrophic) protection failure that results in total compromise of mission capability
• Level II (Critical) protection failure that results in unacceptable compromise of mission capability or significant mission degradation
• Level III (Marginal) protection failure that results in partial compromise of mission capability or partial mission degradation
• Level IV (Negligible) protection failure that results in little or no compromise of mission capability.
[SOWxxx3] For each Level I and Level II Mission-Critical Function identified by the Contractor in the criticality analysis, the Contractor shall identify the associated logic-bearing system components (e.g., HW, firmware, and SW) that implement, protect, or introduce vulnerability, to that function (hereafter referred to collectively as the "critical components").
[SOWxxx4] The Contractor shall demonstrate that the Contractor has mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk

can be introduced through those components, and has implemented or plans to implement countermeasures to mitigate such risks.

[SOWxxx5] The Contractor shall plan for and implement countermeasures that mitigate the risk of foreign intelligence or foreign influence, technology exploitation, supply chain and battlefield threats, and vulnerabilities that result in Level I and Level II protection failures of the system; countermeasures include the following:

1. The application of supply chain risk management best practices, applied as appropriate to the development of the system. Supply chain risk management key practices may be found in the National Institute of Standards and Technology (NIST) Interagency Report 7622, Notional Supply Chain Risk Management for Federal Information Systems (http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf), and the National Defense Industrial Association (2008) guidebook, Engineering for System Assurance, both publicly available (http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf).
2. The enumeration of potential suppliers of critical components, as they are identified, including cost, schedule, and performance information and proposed selection decisions for the purposes of obtaining approval from the Government and engaging in the development of mutually agreeable risk management plans for the selected suppliers of critical components.
3. The processes to control access by foreign nationals to program information, including, but not limited to, system design information, DoD-unique technology, and SW or HW used to integrate commercial technology.
4. The processes and practices employed to ensure that genuine (i.e., not counterfeit) information and communications technology (ICT) are employed in the solution and that processes and requirements for genuine ICT are levied upon Subcontractors. ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., microelectronics, printed circuit boards, computing systems, SW, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in section 11101 of title 40, U.S. Code. Rather, this term reflects the convergence of IT and communications.
5. The processes used to protect both unclassified and classified DoD information, technical data (e.g., source code), and computer SW in the development and support environments (e.g., Government- or Contractor-owned facilities and the integrated development Environment) from entities without a need to know.

APPENDIX D

Appendix D provides individual NAWCTSD Emerging APN Modification OAWR SOW Addendums for projects that have been negotiated and incorporated over contract period of performance in accordance with SOW Section 3.1.4. These SOW Addendums contain the specific Training System Modification requirements including tasks and location(s).